

REMARKS

In response to the Office Action dated September 16, 2005, Applicants respectfully request reconsideration based on the above claim amendments and the following remarks. Applicants respectfully submit that the claims as presented are in condition for allowance.

Applicants have amended independent claims 1 and 24 to include the subject matter of claims 16 and 39, respectively. Accordingly, claims 16 and 39 have been cancelled, and dependent claims 17 and 40 have been amended to adjust dependencies. Applicants submit that no new matter has been introduced by way of the amendments. No new claims have been added. Claims 1-9, 11-14, 17-32, 34-37, and 40-46 remain pending.

Claim Rejections – 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejects claims 1-9, 11-14, 16-32, 34-37, and 39-46 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,983,350 to Minear et al. (“Minear”) in view of U.S. Patent No. 6,799,270 to Bull et al. (“Bull”). Applicants respectfully traverse the rejections.

The Minear reference is directed to a procedure for regulating the flow of messages, both encrypted and not encrypted, over an unprotected network through a firewall. A security association, identified by a security parameter index and a destination IP address, is used to authenticate communication between two firewalls by providing needed processing information to the firewalls. The firewall, acting as a buffer, determines if encrypted and not encrypted messages need to be authenticated. The determination is based upon source and destination addresses, as well as desired services. Authentication protocols include a username/password request and a challenge/response process.

The Bull reference is directed to an authentication protocol used in a network of nodes, in which one node wishes to authenticate communication with a second node. The network includes an authentication server node, which shares a different, secret key with each node of the network. When for example a client node wishes to commence communication with a particular node, the client node sends an authentication request identifying the particular node for which a communication session is sought. This request travels through the network, through one or more intermediate nodes, to the authentication server node. The authentication server node, using secret keys shared with each node, determines if the request

has been altered. If the request has been altered, then communication is not approved. If no alteration to the message has occurred, then the authentication server node generates a response message, to travel through the network by way of the one or more intermediate nodes to the initiating client node. The response message includes a session key as well as a portion of the originating message sent by the client node to alert the client node of its authenticity. Upon receipt of this response message, the client node may use the session key for communicating with the particular node.

Amended claim 1 recites a method for releasing digital content to a rendering application upon authentication of a path, defined by at least one module, between the rendering application and an ultimate destination. The authentication determines if each defining module of the path is to be trusted to handle the digital content. The method claim as amended further recites that the authentication comprises developing a map of each module in the path, receiving a certificate as issued by a certifying authority, determining from the certificate whether the certificate is acceptable, and checking a revocation list to ensure that the certificate has not been revoked. Independent claim 24 recites a computer-readable medium having computer-executable instructions for performing the method of claim 1.

Neither Minear nor Bull, either considered alone or in combination, teach or suggest forwarding decrypted digital content by way of an authenticated path, a feature of both claims 1 and 24. In Minear a path is not authenticated, although packets and a communication session between firewalls may be authenticated. Specifically, messages may be decrypted, but the path through which the messages flow is not authenticated. In Bull, upon a positive determination of an authentication procedure for secure communication, two nodes of a network of nodes may be allowed to securely communicate, but there is no mention of decrypting an encrypted communication once the path has been authenticated, as required by claims 1 and 24.

Furthermore, as Minear does not disclose authenticating a path, there is no teaching or suggestion of a certifying authority issuing a certificate to a module as part of the path authentication process, as recited in amended claims 1 and 24. Also, since Minear does not teach the feature of authenticating a module, there is no suggestion in Minear to use the received certificate to determine authenticity of a module. Bull, in its disclosure of an

authentication procedure, also does not teach or suggest a certifying authority issuing a certificate and then making a determination from the received certificate whether the received certificate is acceptable for authentication purposes. Bull instead discloses an authentication server providing a nested response message to authorize communication if the authentication server has determined that two nodes of a network of nodes may securely communicate.

In addition, as neither Minear nor Bull teach or suggest, either alone or in combination, a certifying authority and a certificate, neither can teach or suggest the step of checking a revocation list to ensure that the received certificate has not been revoked, a feature of amended claims 1 and 24.

Thus, since the combination of Minear and Bull fail to teach or suggest several of the elements of amended claims 1 and 24, as discussed above, a prima facie case of obviousness cannot be established because all elements are not present in any combination of Minear and Bull.

Claims 2-9, 11-14, 17-23 depend on claim 1, while claims 25-32, 34-37, and 40-46 depend on claim 24. These dependent claims (i.e. 2-9, 11-14, 17-23, 25-32, 34-37, and 40-46) are patentable for the same reasons as noted above with respect to claims 1 and 24.

Conclusion

For all the foregoing reasons, Applicants respectfully submit that the pending claims patentably define over the cited art. Accordingly, a Notice of Allowance for claims 1-9, 11-14, 17-32, 34-37, and 40-46 is respectfully requested. In the event, however, that the Examiner believes that the application is not allowable for any reason, the Examiner is encouraged to contact the undersigned agent to discuss resolution of any remaining issues.

Date: December 14, 2005



Erin E. Pacella
Registration No. 56,239

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439